

CONTROL INFORMATION REWRITING SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

This application is based on and incorporates herein
5 by reference Japanese Patent Application No. 11-347562 filed
December 7, 1999.

BACKGROUND OF THE INVENTION

10 This invention relates to an electronic control
information rewriting system having nonvolatile memory with
which electrical rewriting of data is possible, and particularly
relates to technology for preventing the illegitimate rewriting
of control information such as vehicle control programs or
control data stored in the nonvolatile memory.

15 In electronic control units (ECUs) for controlling
vehicle engines or the like, control information is stored in
a nonvolatile memory with which electrical rewriting of data is
possible. The control information includes programs and data
and is rewritable even in the market after production.

20 For instance, this kind of ECU is constructed as shown
in Fig. 9. A rewriting device 200 is connected to a vehicle 100
via a vehicle diagnosis connector 120. A plurality of ECUs 101,
102, 103 and 104 are mounted in the vehicle 100, and the ECUs
101 through 104 are connected by a network line 110. The
25 rewriting device 200 performs data communication with one of the
four ECUs 101 through 104 by transmitting each ECU code on the
basis of a manipulation of an operator.

In this system, as shown in Fig. 10, the rewriting device 200 selects the ECU 101, for instance, on which rewriting of control information is to be carried out, and transmits a rewriting request (b1). The selection of the ECU 101 is carried out by transmitting an ECU code. This ECU code is inputted to the rewriting device 200 by an operator. When this is done, the selected ECU 101 generates a random number r (b2), and transmits this random number r to the rewriting device 200 (b3).

A function f is pre-stored in the rewriting device 200, and it calculates a function value $f(r)$ with respect to the transmitted random number r (b4). Then, it transmits this calculated function $f(r)$ (b5). In the ECU 101, on the other hand, a function F is pre-stored, and a function value $F(f(r))$ is calculated with respect to the transmitted function value $f(r)$ (b6). Then, if the calculated $F(f(r))$ corresponds to the random number r , that is if $f=F^{-1}$, it transmits a permission signal permitting rewriting (b7).

The above processing is for the ECU 101 to determine that the rewriting device 200 is legitimate when the rewriting device 200 has the inverse function f of the function F stored by the ECU 101.

The rewriting device 200, when receiving the permission signal transmitted from the ECU 101 (b8), transmits modification data. The ECU 101 carries out rewriting of control information on the basis of this modification data (b10). When the rewriting of control information completes normally, the ECU reports normal completion (b11), and the rewriting device

receives the report (b12) and one chain of rewriting processing ends.

In the above rewriting processing by communication processing (b1 through b7) using the function f, which is information inside the rewriting device 200, each ECU determines the legitimacy of the rewriting device 200. As a result, when the rewriting device 200 itself is stolen or information inside the rewriting device 200 is stolen, illegitimate rewriting of control information cannot be prevented. In particular, because the rewriting device 200 is provided, for instance, at a work site such as a car dealer, the possibility of the above theft is relatively high.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to prevent illegitimate rewriting of control information even when a rewriting device or information inside a rewriting device is stolen.

According to the present invention, a control information rewriting system has a control center as an external device for conducting data communication with a rewriting device. The control center could for example be installed in a different place from a rewriting work site. Access information is stored in the control center. Identification information and associated information are stored in the rewriting device. Identification information could be a number or the like unique to the rewriting device for identifying the rewriting device.

Associated information is information set in association with identification information.

For the legitimacy determination, the control center acquires the identification information and the associated information of the rewriting device in data communication with the rewriting device. Then, when an association relationship of the acquired information matches an association relationship, it transmits predetermined access information to the rewriting device. On the other hand, when it does not match, the predetermined access information is not transmitted to the rewriting device.

That is, the system attains the following two-stage checks.

[1] The control center determines the legitimacy of the rewriting device and transmits access information to the rewriting device.

[2] The rewriting device executes communication start processing using that access information, and each electronic control unit determines the legitimacy of the rewriting device on the basis of that communication start processing.

Thus, if at least either one of the identification information or the associated information is not pre-stored inside the rewriting device, the rewriting device cannot obtain access information from the control center. Therefore, if the rewriting device or information inside the rewriting device is stolen, it is not determined by the electronic control unit that the rewriting device is legitimate. Thus, rewriting of control

information is not carried out. As a result, even when the rewriting device or information inside the rewriting device is stolen, it is possible to prevent control information of an electronic control unit being improperly rewritten.

5

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the present invention will become more apparent from the following detailed description made with reference to the accompanying drawings. In the drawings:

10

Fig. 1 is a block diagram showing a control information rewriting system according to an embodiment of the present invention;

Fig. 2 is an operation diagram showing rewriting processing in the embodiment;

15

Fig. 3 is a flow diagram showing a first half of ECU side processing in the embodiment;

Fig. 4 is a flow diagram showing a second half of ECU side processing in the embodiment;

20

Fig. 5 is a flow diagram showing a first half of rewriting device side processing in the embodiment;

Fig. 6 is a flow diagram showing a second half of rewriting device side processing in the embodiment;

25

Fig. 7 is a flow diagram showing a first half of control center side processing in the embodiment;

Fig. 8 is a flow diagram showing a second half of control center side processing in the embodiment;

Fig. 9 is a block diagram showing a control information rewriting system according to a related art; and

Fig. 10 is an operation diagram showing rewriting processing in the related art.

5

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

An embodiment of the present invention will now be described with respect to rewriting of vehicle control information.

10

Referring first to Fig. 1, a plurality of ECUs 11, 12, 13 and 14 are mounted in a vehicle 10, and the ECUs 11 through 14 are connected by a network line 15. The ECUs 11 through 14 have respective EEPROMs 11a through 14a which are nonvolatile type. At normal time, when a rewriting device 20 is not connected, on the basis of control information (control programs and control data) stored in this EEPROM, carry out communication between the ECUs 11 through 14 via the network line 15, and control respective control objects such as an engine.

15

20

In Fig. 1, the rewriting device 20 is shown as connected by way of a vehicle diagnosis connector 16 to the ECUs 11 so that a control information rewriting system 1 is formed. The vehicle diagnosis connector 16 is a connector provided on the vehicle 10 for making possible data communication between the rewriting device 20 and the ECUs 11 through 14 via the network line 15.

25

The vehicle 10 and the rewriting device 20 are installed in a work site such as a car dealer or repair shop.

In the control information rewriting system 1 of this

embodiment, the rewriting device 20 is capable of data communication via a telephone line network 40 with a control center 30. The control center 30 is installed as a so-called server as an external device in a different location from the work site. In a storage device (memory) 31 of this control center 30, access information for the rewriting device 20 to access the ECUs 11 through 14 with, modification data for rewriting or modifying control information, a database for determining the legitimacy of the rewriting device 20, and a database of control information update histories of different vehicles 10 are stored.

When the rewriting device 20 calls the control center 30, predetermined communication processing is carried out between the rewriting device 20 and the control center 30. The rewriting device 20 and the control center 30 assume a state such that data communication is possible. In Fig. 1, the control center 30 is shown as connected to a single rewriting device, but it is also conceivable for example for a rewriting device of a different work site to be connected to the control center 30 in parallel.

In this embodiment, the rewriting device 20 may be a portable personal computer which can be used for any types of vehicles. The control center 30 may be managed by a car manufacturer. The rewriting device 20 may be connected with the control center 30 by way of other means, for instance, cable TV network or wireless phone network, in place of ground telephone line network 40.

The operation of this control information rewriting system 1 is shown in block units B1 through B18. The processing in the ECUs 11 through 14 is shown as ECU side processing in a left side column in Fig. 2 as B5, B6, B9, B10, B15 and B16. The processing in the rewriting device 20 is shown as rewriting device side processing in a central column as B1, B4, B7, B8, B11, B14 and B17. The processing in the control center 30 is shown as control center side processing in a right side column as B2, B3, B12, B13 and B18. These processing are executed in the order B1 → B2 → B3 → ... → B18.

In operation, the rewriting device 20 first calls the control center 30. When a data communication possible state is established between the rewriting device 20 and the control center 30, the rewriting device 20 transmits to the control center 30 ID information as identification information for identifying the rewriting device 20 itself together with a communication start request (B1). With respect to this, the control center 30 receives the ID information from the rewriting device 20 and acquires the telephone number of the call origin, that is, the telephone number of the rewriting device 20 (B2). This telephone number is associated information.

The control center 30 has a database wherein the ID information of the rewriting device 20 and a telephone number assigned to the rewriting device 20 are associated. Accordingly, the control center 30 compares the association relationship between the received ID information and the acquired telephone number with an association relationship in the database (B2).

If they match, it transmits a first permission signal and a function f to the rewriting device 20 (B3).

The rewriting device 20 selects an ECU to be the object of control information rewriting from among the ECUs 11 through 14, and transmits a rewriting request to that ECU (B4). It is assumed here that the ECU 11 has been selected as the ECU to be the object of control information rewriting. The selected ECU 11 generates a random number r (B5) and transmits this random number r to the rewriting device 20 (B6).

The rewriting device 20, using the function f transmitted to it from the control center in B3 above, calculates a function value $f(r)$ with respect to the random number r from the ECU 11 (B7). Then, it retransmits this calculated function value $f(r)$ to the ECU 11 (B8).

On the other hand, a function F is pre-stored in the ECU 11, and with respect to the function value $f(r)$ transmitted from the rewriting device 20 it calculates a function value $F(f(r))$ (B9). Then, if the calculated function value $F(f(r))$ corresponds to the random number r , that is if $f = F^{-1}$, it transmits a second permission signal permitting rewriting and transmits a vehicle VIN code (B10). The vehicle VIN code is a number assigned uniquely to each vehicle, and this corresponds to the above vehicle information.

The rewriting device 20 receives the second permission signal and the vehicle VIN code from the ECU 11 and transmits these information on to the control center 30 (B11).

The control center 30 has respective control

information update histories of each vehicle as a database. Accordingly, on the basis of the vehicle VIN code from the rewriting device 20, it carries out distinguishing of the vehicle 10, refers to the update history database, and determines the necessity of rewriting of control information (B12). When it determines that rewriting of control information to the vehicle 10 is necessary, it transmits modification data to the rewriting device 20 (B13).

The rewriting device 20 receives the modification data from the control center 30 and transmits this modification data to the ECU 11 (B14). The ECU 11, on the basis of the modification data from the rewriting device 20, performs rewriting of control information (B15). Then, if the rewriting of control information ends normally, it reports normal ending to the rewriting device 20 (B16). The rewriting device 20, when normal ending is reported from the ECU 11, erases the function f transmitted to it from the control center 30 in B3 above (B17). It reports normal ending to the control center 30. On the basis of this, the control center 30 updates the update history database (B18).

It is preferable that the functions $f(r)$ and $F(f(r))$ are differentiated from vehicle type to vehicle type from the standpoint of security.

For the above processing, the ECUs 11 through 14, the rewriting device 20 and the control center 30 are programmed to operate as shown in Figs. 3 through 8.

The ECU side processing executed in the ECUs 11 through 14 will be explained with reference to Figs. 2 and 3. This ECU

side processing is executed, with the rewriting device 20 connected by way of the vehicle diagnosis connector 16 to the vehicle 10, at a predetermined time interval such as for example 0.2 seconds.

5 First, at step (S) 300, it is determined whether or not there was a rewriting request from the rewriting device 20. When it is determined that there was a rewriting request (S300: YES), processing proceeds to S310. When on the other hand it is determined that there was not a rewriting request (S300: NO), this ECU side processing is terminated.

At S310, it is determined whether or not an access refusal timer is 0. The access refusal timer is set when it is determined a predetermined number of times in succession that the rewriting device 20 is not legitimate, as described above. When it is determined that the access refusal timer is not 0 (S310: NO), the timer is decremented at S320, and 0 is assigned to a variable C1, and this ECU side processing is terminated. The variable C1 counts the number of times in succession it is determined that the rewriting device is not legitimate. On the other hand, when it is determined that the access refusal timer is 0 (S310: YES), processing proceeds to S330.

At S330, it is determined whether or not the variable C1 is not greater than 2. When here $C1 > 2$ (S330: NO), at S340 the access refusal timer is set and this ECU side processing is terminated. In this embodiment, 10 minutes is set. On the other hand, when $C1 \leq 2$ (S330: YES), processing proceeds to S350.

At S350, a random number r is generated, and

transmitted to the rewriting device 20. This processing corresponds to the processing of B5 and B6 in Fig. 2. With respect to this, as shown in B8 in Fig. 2, a function value $f(r)$ is transmitted from the rewriting device 20.

5 Accordingly, At the following S360, it is determined whether or not there was transmission of a function value $f(r)$. When here there was transmission of a function value $f(r)$ (S360: YES), processing proceeds to S370. On the other hand, as long as there is no transmission of a function value $f(r)$ (S360: NO), this determination processing is repeated.

 At S370, with respect to the function value $f(r)$ transmitted from the rewriting device 20, a function value $F(f(r))$ is calculated. This processing corresponds to the processing of B9 in Fig. 2.

 At the following S380 of Fig. 4, it is determined whether or not the calculated function value $F(f(r))$ corresponds to the random number r . When here $F(f(r)) = r$ (S380: YES), at S390 the second permission signal and the vehicle VIN code are transmitted, and processing proceeds to S420. The processing of S380 and S390 corresponds to the processing of B10 in Fig. 2. On the other hand, when $F(f(r)) \neq r$ (S380: NO), it is reported at S400 to the rewriting device 20 that rewriting is not permitted, and at S410 the variable C1 is incremented and this ECU side processing is terminated. In this way the legitimacy of the rewriting device 20 is determined. When it is determined to be not legitimate (S380: NO), the variable C1 is incremented (S410), and at $C1 > 2$ the timer is set as described above (S340

in Fig. 2). Thus, in this embodiment, when it is determined three times in succession that the rewriting device 20 is not legitimate, by C1 0 → 1 → 2, access refusal is carried out.

By the control center 30 a control information
5 rewriting necessity determination based on the vehicle VIN code is carried out. If rewriting is necessary modification data is transmitted from the control center 30 via the rewriting device 20. On the other hand, if rewriting is not necessary, that is, when rewriting of control information has been carried out already, information indicating that rewriting has been done is transmitted from the control center 30 via the rewriting device
10 20.

For this, at S420, it is determined whether or not there was data transmission from the rewriting device 20. When it is determined that there was data transmission (S420: YES),
15 processing proceeds to S430. On the other hand, as long as there is no data transmission (S420: NO), this determination processing is repeated.

Then, at S430, it is determined whether or not the data
20 transmitted from the rewriting device 20 is modification data. When it is determined that it is modification data (S430: YES), processing proceeds to S440. On the other hand, when it is determined that it is not modification data (S430: NO), that is, when information indicating that rewriting has been done was
25 transmitted, the subsequent processing is not executed and this ECU side processing is terminated.

At S440, on the basis of the transmitted modification

data, rewriting of control information is carried out. At the following S450, a post-rewriting check sum of control information is calculated. This is for determining whether or not the control information was rewritten normally.

5 Then, at the next S460, on the basis of the check sum calculated at S450, it is determined whether or not the rewriting of control information ended normally. When it is determined that it ended normally (S460: YES), at S470 normal ending is reported to the rewriting device 20, and after that this ECU side processing is terminated. On the other hand, when it is not determined that it ended normally (S460: NO), at S480 the rewriting device 20 is requested to retransmit the modification data, and the processing from S420 is repeated.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
9460
9465
9470
9475
9480
9485
9490
9495
9500
9505
9510
9515
9520
9525
9530
9535
9540
9545
9550
9555
9560
9565
9570
9575
9580
9585
9590
9595
9600
9605
9610
9615
9620
9625
9630
9635
9640
9645
9650
9655
9660
9665
9670
9675
9680
9685
9690
9695
9700
9705
9710
9715
9720
9725
9730
9735
9740
9745
9750
9755
9760
9765
9770
9775
9780
9785
9790
9795
9800
9805
9810
9815
9820
9825
9830
9835
9840
9845
9850
9855
9860
9865
9870
9875
9880
9885
9890
9895
9900
9905
9910
9915
9920
9925
9930
9935
9940
9945
9950
9955
9960
9965
9970
9975
9980
9985
9990
9995
10000
10005
10010
10015
10020
10025
10030
10035
10040
10045
10050
10055
10060
10065
10070
10075
10080
10085
10090
10095
10100
10105
10110
10115
10120
10125
10130
10135
10140
10145
10150
10155
10160
10165
10170
10175
10180
10185
10190
10195
10200
10205
10210
10215
10220
10225
10230
10235

following S510, it is determined whether or not there was a response from the control center 30. When it is determined that there was a response from the control center 30 (S510: YES), processing proceeds to S520. On the other hand, as long as there is no response from the control center 30 (S510: NO), this determination processing is repeated.

At S520, it is determined whether or not the response of the control center 30 is a report of non-permission. When it is determined that it is a report of non-permission (S520: YES), at S530 it is displayed on a display device such as a display that there has been a failure to access the control center 30. After that, the processing from S500 is repeated. On the other hand, when it is not a report of non-permission (S520: NO), that is, when the first permission signal and the function f have been transmitted, processing proceeds to S540.

At S540, the input of an ECU code for selecting one of the four ECUs 11 through 14 mounted in the vehicle 10 is requested of the operator. At the following S550, it is determined whether or not there was the input of an ECU code. When it is determined that there was the input of an ECU code (S550: YES), processing proceeds to S560. On the other hand, as long as there is no input of an ECU code (S550: NO), the processing from S540 is repeated. The following description will be continued assuming that the ECU code of the ECU 11 was inputted.

At S560, a rewriting request and the ECU code are transmitted. This processing corresponds to the processing of B4 in Fig. 2. On the basis of this, the ECU 11 generates a random

number r and transmits that random number r (S350 in Fig. 3).

Accordingly, at the following Step S570, it is determined whether or not a random number r has been transmitted. When it is determined that a random number r has been transmitted (S570: YES), processing proceeds to S580. On the other hand, as long as no random number r is transmitted (S570: NO), this determination processing is repeated.

At S580, using the function f transmitted from the control center 30 at S510, a function value $f(r)$ specific to the random number r is calculated. At the next S590, the function value $f(r)$ is transmitted to the ECU 11. This corresponds to the processing of B7 and B8 in Fig. 2.

With respect to this, in the ECU 11, an affirmative determination is made at S360 in Fig. 3, and the function value $F(f(r))$ is calculated (S370). Then, on the basis of the determination of S380, transmission of a second permission signal or reporting that rewriting will not be permitted is carried out (S390, S400).

Accordingly, at the following S600 of Fig. 6, it is determined whether or not there was a response from the ECU 11. When it is determined that there was a response of the ECU 11 (S600: YES), processing proceeds to S610. On the other hand, as long as there is no response from the ECU 11 (S600: NO), this determination processing is repeated.

At S610, it is determined whether or not a second permission signal was transmitted from the ECU 11. When it is determined that a second permission signal was transmitted

(S610: YES), at S620 the second permission signal and the vehicle VIN code transmitted together with that second permission signal are transmitted to the control center 30, and after that processing proceeds to S640. This processing corresponds to the processing of B11 in Fig. 2. On the other hand, when a second permission signal was not transmitted (S610: NO), that is, when it was reported from the ECU 11 that rewriting will not be permitted, at S630 it is reported to the control center 30 that permission has not been given, and after that, processing proceeds to S530 in Fig. 5.

When at S620 the second permission signal and the vehicle VIN code are transmitted to the control center 30, the control center 30 determines the necessity of rewriting. If there is a need for rewriting, the control center 30 transmits modification data. On the other hand, if there is no need for rewriting, the control center 30 transmits information indicating that rewriting has been done.

Accordingly, at S640, it is determined whether or not there was a response from the control center 30. When it is determined that there was a response from the control center 30 (S640: YES), processing proceeds to S650. On the other hand, as long as there is no response (S640: NO), this determination processing is repeated.

At S650, it is determined whether or not the data transmitted from the control center 30 is modification data. When it was modification data (S650: YES), processing proceeds to S680. On the other hand, when it is not modification data

(S650: NO, that is, when information indicating that rewriting has been done was transmitted from the control center 30, the function f is erased and it is displayed that there is no need for rewriting (S660). Information indicating that rewriting has been done is transmitted to the ECU 11 (S670). This rewriting device side processing is then terminated.

At S680, the modification data transmitted from the control center 30 is transmitted to the ECU 11. This processing corresponds to the processing of B14 in Fig. 2. On the basis of this, in the ECU 11 rewriting of control information is carried out (S430 in Fig. 4: YES, S440), and a report of normal ending or a re-transmission request is transmitted from the ECU 11 (S470, 480).

Accordingly, at the next S690, it is determined whether or not there was a report of normal ending from the ECU 11. When it is determined that there was a report of normal ending (S690: YES), the function f is erased and normal ending is reported to the control center 30 (S700), and after that this rewriting device side processing is terminated. On the other hand, when there was not a report of normal ending (S690: NO), that is, when there was a request for re-transmission of the modification data, abnormal ending is reported to the control center 30 (S710) and this rewriting device side processing is terminated.

Continuing further, on the basis of the flow diagram of Fig. 7 and Fig. 8, the control center side processing executed by the control center 30 will be described. This control center side processing is executed, with a data communication possible

state established between the rewriting device 20 and the control center 30, at a predetermined time interval such as for example 0.2 seconds.

First, at S800, it is determined whether or not the access refusal timer is 0. The access refusal timer is set when it is determined a predetermined number of times in succession by the control center 30 that the rewriting device 20 is not legitimate, as will be further discussed later. When it is determined that the access refusal timer is not 0 (S800: NO), at S810 the timer is decremented. Further, 0 is assigned to a variable C2, and this control center side processing is terminated. The variable C2 counts the number of times in succession it is determined by the control center 30 that the rewriting 20 is not legitimate. On the other hand, when it is determined that the access refusal timer is 0 (S800: YES), processing proceeds to S820.

At S820, it is determined whether or not the variable C2 is not greater than 2. When here $C2 > 2$ (S820: NO), at S830 the access refusal timer is set, and after that, this control center side processing is terminated. On the other hand, when $C2 \leq 2$ (S820: YES), processing proceeds to S840.

At S840, it is determined whether or not there was a communication start request. This processing is specific to the processing of S500 in Fig. 5. When it is determined that there was a communication start request (S840: YES), processing proceeds to S850. On the other hand, as long as there is no communication start request (S840: NO), this determination

processing is repeated.

At S850, the ID information transmitted from the rewriting device 20 is received and the telephone number of the call origin is acquired. At the following S860, the association relationship between the received ID information and the acquired telephone number is compared with the association relationship between the ID information and the telephone number of the rewriting device 20 pre-stored in the database. The processing of these S850 and S860 corresponds to the processing shown in B2 of Fig. 2.

Then, at the next S870, on the basis of the comparison result, it is determined whether or not the association relationships match. When it is determined that they matched (S870: YES), at S890 the first permission signal and the function f are transmitted, and after that, processing proceeds to S900. This processing corresponds to the processing of B3 in Fig. 2. On the other hand, when it is determined that they did not match (S870: NO), it is reported to the rewriting device 20 that rewriting will not be permitted, and the variable C2 is incremented (S880), and after that, the processing from S800 is repeated.

The processing of S850 to S890 explained here corresponds to processing serving as legitimacy determining means. Therefore, the CPU of the control center 30 thus executes legitimacy determination.

When the first permission signal and the function f are transmitted, the rewriting device 20 transmits back the second

permission signal and the vehicle VIN code (S620 in Fig. 6), or reports the non-permission of rewriting (S630).

Accordingly, at S900, it is determined whether or not there was a response from the rewriting device 20. When it is determined that there was a response from the rewriting device 20 (S900: YES), processing proceeds to S910 in Fig. 8. On the other hand, as long as there is no response from the rewriting device 20 (S900: NO), this determination processing is repeated.

At S910, it is determined whether or not that response is a report of non-permission. When it was a report of non-permission (S910: YES), processing proceeds to S800 in Fig. 7. On the other hand, when it is not a report of non-permission (S910: NO), that is when the second permission signal and the vehicle VIN code were transmitted, processing proceeds to S920.

At S920, distinguishing of the vehicle is carried out on the basis of the transmitted vehicle VIN code, and the update history database is referred to. Then, at the next S930, on the basis of the reference result, it is determined whether or not there is a need to rewrite control information. The processing of these S920 and S930 corresponds to B12 in Fig. 2. When it is determined that there is a need of rewriting (S930: YES), processing proceeds to S950. On the other hand, when it is determined that there is no need of rewriting (S930: NO), at S940 information indicating that rewriting has been done is transmitted, and after that, this control center side processing is terminated.

At S950, modification data is searched for and read

out, and the modification data read out is transmitted to the rewriting device 20. This processing corresponds to the processing of B13 in Fig. 2. After that, from the rewriting device 20, as described above there is a report of normal ending (S700 in Fig. 6) or a report of abnormal ending (S710).

Accordingly, at S960, it is determined whether or not there was an ending report from the rewriting device 20. When it is determined that there was an ending report (S960: YES), processing proceeds to S970. On the other hand, as long as there is no ending report (S960: NO), this determination processing is repeated.

At S970, it is determined whether or not the ending report is a report of normal ending. When it is determined that it is a report of normal ending (S970: YES), at S980 the update history database is updated, and after that, this control center side processing is terminated. On the other hand, when it is determined that it is not a report of normal ending (S970: NO), that is, when it was a report of abnormal ending, the processing from S950 is repeated.

According to the above embodiment, the function f constituting access information is stored in the control center 30. Only when the control center 30 determines the rewriting device 20 to be a legitimate one, the function f is transmitted from the control center 30 to the rewriting device 20 (B2, B3 in Fig. 2). Therefore, even when the rewriting device 20 or information inside the rewriting device 20 is stolen, the access information for accessing the ECUs 11 through 14 is not stored

in the rewriting device 20. Therefore, it is not possible to rewrite the control information of the ECUs 11 through 14, if it is not possible to obtain access information from the control center 30.

5 The control center 30 has a database in which ID information uniquely assigned to the rewriting device 20 and a telephone number of the rewriting device 20 side of when data communication is to be carried out via a telephone line are stored in association. It acquires ID information from the rewriting device 20 and acquires the telephone number from which the call was made (S850 in Fig. 7). When the association relationship between this ID and telephone number matches the association relationship stored in the database (S860, S870: YES), the control center 30 determines that the rewriting device 20 is legitimate and transmits the function f, which is access information (S890). For example when a line is connected between the rewriting device 20 and the control center 30 from other than a regular work site, the telephone number that the control center 30 acquires ceases to be the pre-decided telephone number. Consequently, it does not correspond with the ID information, and the access information cannot be obtained from the control center 30. As a result, it is not possible to rewrite the control information in the ECUs 11 through 14.

As described above, with the control information rewriting system 1 of this embodiment, even when the rewriting device 20 or information inside the rewriting device 20 is stolen, control information of the ECUs 11 through 14 being

improperly rewritten can be certainly prevented.

With the control information rewriting system 1 of this embodiment, the control center 30 firstly determines the legitimacy of the rewriting device 20 and then the ECUs 11 through 14 determine the legitimacy of the rewriting device 20. When in either of these checks of two stages it is determined three times in succession that the rewriting device 20 is not legitimate, a ten minute access refusal is carried out.

That is, in the ECUs 11 through 14, when it is determined that the rewriting device 20 is not legitimate (S380: NO in Fig. 4), the variable C1 is incremented (S410). When the variable C1 becomes larger than 2 (S330: NO in Fig. 3), that is, when a determination of not legitimate is made three times in succession, an access refusal timer is set (S340). Thus, access of the rewriting device 20 is refused (S310: NO) until the timer becomes 0.

Meanwhile, similarly in the control center 30 also, when it is determined that the rewriting device 20 is not legitimate (S870: NO in Fig. 7), the variable C2 is incremented (S880). When the variable C2 becomes larger than 2 (S820: NO), that is, when a determination of not legitimate is made three times in succession, an access refusal timer is set (S830). Thus, access of the rewriting device 20 is refused (S800: NO) until the timer becomes 0.

As a result, even when an attempt is made to access the control center 30 or the ECUs 11 through 14 from the rewriting device 20 using illegitimate information, the control

information rewriting prevention can be prevented. Because it is not possible to access many times in succession, for the reason that access becomes impossible for ten minutes, if illegitimate access is carried out three times in succession.

5 In this embodiment, the control center 30 stores modification data of control information. That is, because modification data is not stored in the rewriting device 20 as in the past, even when the rewriting device 20 or information inside the rewriting device 20 is stolen, there is no possibility of modification data leaking to outside.

10 The control center 30 transmits modification data (S950) with a second permission signal from the ECUs 11 through 14 having been transmitted to it as one condition (S910: NO). That is, it transmits modification data with it having been determined by the ECUs 11 through 14 that the rewriting device 20 is legitimate as a condition. Therefore, the possibility of modification data leaking to outside is further reduced.

15 When the ECUs 11 through 14 determine that the rewriting device 20 is legitimate (S380: YES in Fig. 4), in addition to the second permission signal, they transmit a vehicle VIN code with which it is possible to specify the vehicle 10 (S390). The control center 30 has a database of update histories of control information stored in the ECUs 11 through 14 of different vehicles 10, and on the basis of the above-mentioned vehicle VIN code from the ECUs 11 through 14, distinguishes the vehicle 10 and refers to the database (S920 in Fig. 8) and determines the necessity of control information rewriting

(S930). Then, when there is a need of rewriting (S930: YES), it transmits the modification data (S950).

In this embodiment, because the control center 30 manages the control information update histories of vehicles 10, futile rewriting of control information is not carried out. As a result, futile work time is not needed, and it ceases to happen that a necessary rewriting becomes impossible due to futile rewriting.

In the control center 30, when normal ending of rewriting is reported from the ECUs 11 through 14 via the rewriting device 20 (S970: YES in Fig. 8), the control information update history database is updated automatically (S980). Thus, there is no need for an operator to update the database by a manual operation.

In the rewriting device 20, when the function f constituting access information ceases to be needed (S650: NO, S690: YES in Fig. 6), that function f constituting access information is swiftly erased (S660, S700). Because of this, the possibility of the function f serving as access information transmitted from the control center 30 to the rewriting device 20 being stolen from the rewriting device 20 can be reduced.

This invention is not limited in any way to the disclosed embodiment, but may be implemented in other ways without departing from the spirit of the invention as follows.

(1) The control center 30 may have a database wherein the ID information of rewriting devices 20 and passwords are associated, and the rewriting device 20 may transmits a password

inputted by an operator together with the ID information. In this case, the password corresponds to associated information, and the control center 30 determines the legitimacy of the rewriting device 20 on the basis of the correspondence between the ID information and the password transmitted from the rewriting device 20.

The ID information may also be inputted from a user in the same way as the password. If this is done, even when the rewriting device 20 or information inside the rewriting device 20 is stolen, because the password or the ID information and the password are not known, it is not possible to obtain access information from the control center 30, and it is possible to prevent the improper rewriting of control information in the same way as in the embodiment described above.

However, because there is also a possibility of the ID information or the password being stolen by some other route, it is preferable for a telephone number connected with the installation site of the rewriting device 20 to be made associated information as in the embodiment described above. This is because improper rewriting is not carried out at a regular work site.

(2) It is conceivable for data communication between the control center 30 and the rewriting device 20 to be ended temporarily after the rewriting device 20 acquires the access information from the control center 30. For example, it is conceivable for data communication to be temporarily ended after the data communication of B1 through B4 in Fig. 2 finishes and

for a data communication possible state between the rewriting device 20 and the control center 30 to be re-established when the processing of B11 onwards is carried out.

However, there is a possibility of access information transmitted to the rewriting device 20 being stolen and the ECUs 11 through 14 being accessed using this access information, using a different rewriting device.

Therefore, it is beneficial if the control center 30 and the rewriting device 20 being in a data communication possible state is made a condition of rewriting until the chain of rewriting processing (the processing of B1 through B18 shown in Fig. 2) ends.

Specifically the following kind of construction could be adopted. That is, the rewriting device 20 may regularly transmit a response request to the control center 30 on the basis of timer interrupt processing or the like, and the control center 30 may perform a response. At this time, when there has ceased to be a response from the control center 30 before the chain of rewriting processing completes, the rewriting device 20 does not perform rewriting of the ECUs 11 through 14. If this is done, it becomes impossible to access an ECU from a different rewriting device using stolen access information.

(3) In the case where control programs stored in the ECU 11 becomes out of order for some reason, the processing shown in Fig. 2 should be modified so that such control programs may be rewritten.

In this instance, after executing B1 through B9 in Fig.

2, the ECU 11 reads out check sum of its control program and transmits it to the rewriting device 20 along with the second permission signal and the VIN code (B10). The rewriting device 20 transmits those received information to the control center 30 (B11). The control center 30 determines whether it is necessary to rewrite the control program based on the comparison of VIN code and check sum between the received ones and the pre-stored ones (12). Specifically, the control center 30 determines the version of the control program in the ECU 11 based on the received VIN code and determines whether the control program is normal by checking the received check sum of the control program. If the check sum differs from the pre-stored value, it determines that the control program is out of order or broken.

If the control center 30 determines based on the VIN code that the version of the control program has been changed, it transmits the modification data to the rewriting device 20 irrespective of the check sum determination result (B13). If the control center 30 determines that the version of the control program has not been changed but the control program is out of order, it transmits the original control program to the rewriting device 20. Thus, the control program in the ECU 11 can be renewed. It is of course possible to use key words or the like provided within the control program in place of using the check sum for detecting whether the control program has become out of order.